Security Risk Report

Prepared for Company A

Tuesday 07 October 2015

Prepared by Mike Storm, Cisco Preferred Partner

Contact: partner_se@company.com

Network Risk Report

Prepared for Company A

Tuesday 07 October 2015

Prepared by Mike Storm, Cisco Preferred Partner

Contact: partner_se@company.com

I. EXECUTIVE SUMMARY

Cisco has determined that Company A is at a High risk due to the use of applications that are potentially dangerous to the enterprise yet have low business relevance. These applications may leave your network vulnerable to attack, carry malware, or waste bandwidth.

Assessment Period: Tue Sep 23 15:52:26 2014 to Tue Oct 7 15:52:26 2014

Risky Apps	Risky Users	High Bandwidth Apps
21	*	53
Encrypted Apps	**Evasive Apps**	**Dangerous Web Browsers**
107	9	2792

* AD Integration disabled

(A summary of the assessment results starts on page 3)

YOUR NETWORK PROFILE

26	0	1381	42
Operating Systems	Mobile Devices	Applications In Use	File types transferred

RECOMMENDATIONS

Cisco recommends Company A deploy Cisco FirePOWER Appliances (NGIPS/NGFW) with App Control and URL Filtering to:

1. Reduce your application attack surface
2. Granularly control applications, bandwidth, URL access and acceptable use policies
3. Get visibility into network risks and usage, including mobile devices and BYOD risk

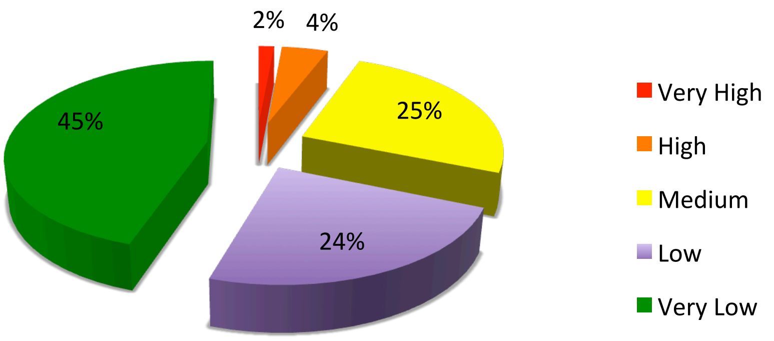
II. APPLICATION RISK

APPLICATIONS WITH HIGH RISK AND LOW BUSINESS RELEVANCE

Some applications carry high risk because they can be vectors for malware into the organization, possess recent vulnerabilities, use substantial network resources, or hide the activities of attackers. Other applications have low business relevance: they are not relevant to the activities of a typical organization. When an application has high risk and low business relevance, it is a good candidate for application control to reduce your application risk. You should investigate these applications to determine whether they are important to control.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
MySpace	1,879	Very High	Very Low	21.72
ICA	146	Very High	Very Low	36.15
Gnutella	4	Very High	Very Low	0.03
BitTorrent	3	Very High	Very Low	0.01
The Pirate Bay	2	Very High	Very Low	0.04

SUMMARY OF ALL NETWORK CONNECTIONS BY APPLICATION RISK



HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
YouTube	107,371	High	Very Low	17,427.27
Microsoft Update	200,412	Medium	Low	15,851.20
SymantecUpdates	55,530	Medium	Low	14,614.18
MP4	1,519	Very Low	Medium	4,966.72
MPEG	2,922	Low	Medium	4,319.68

ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
Microsoft CryptoAPI	1,699,263	Medium	Medium	14,272.57
FTP Data	1,226,928	Medium	Medium	83,266.07
Facebook	1,086,484	Very High	Low	4,826.27
Outlook	401,759	High	Medium	2,796.36
Amazon	384,476	Very Low	Low	7,217.45

EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
BitTorrent	3	Very High	Very Low	0.01
Skype	2,120	Very High	Medium	12.59
Hideman Login	1,062	Very High	Medium	5.72
Infonline	6	Very High	Medium	0.01
Hotspot Shield	155	High	Low	2.69

OTHER APPLICATIONS OF INTEREST

Other applications were observed that may be of interest and possibly candidates for control. Users may use anonymizers and proxies to bypass your network security or cloak their identities. Gaming applications may be distractions to productivity and use excessive bandwidth. Peer-to peer applications are often malware vectors. And remote administration applications may allow malicious users to control machines in your environment.

Anonymizers and Proxies (accesses):

Squid(191) , Freenet(66) , Hotspot Shield(9) , SOCKS(3) , Avocent(2)

Games and Recreation (accesses):

Facebook(1929) , Scorecard Research(627), Twitter(624), Quantcast(620), Google+(609), BlueKai(566), Google+(609), BlueKai(566),

Peer-to-Peer and Sharing (accesses):

MSN(336), cURL(336), MS Online(336), Windows Live(321), Skype Tunneling(286), Pinterest(269), Windows Media Player(268),

Remote Administration and Storage (accesses):

SSH(851) , Telnet(649) , TN3270(649) , syslog(518) , RADIUS-acct(461) , RADIUS(411) , RDP(366) , RDP(366) , FTP Data(336) ,

DANGEROUS WEB BROWSER VERSIONS

A profile of your network revealed the following old web browsers in use. Outdated web browsers are a major vector for network malware and it is important to update them (or encourage users to). These browsers often have unpatched vulnerabilities or carry other risks.

BROWSER	VERSION	NUMBER OF HOSTS
Internet Explorer	5.5, 6, 6.0 (Compat), 7, 7.0 (Compat)	2718
Chrome		0
Safari		0
Firefox	12, 14.0.1, 15, 16, 2.0.0.16	74

RISKY WEB BROWSING

The following web communications were identified that correspond to risky activity. Malware sites, open proxies and anonymizers, keyloggers, phishing sites, and spam sources are all Web activities that can put your networks at risk. It is wise to evaluate the use of URL filtering technologies to detect and control communications to risky sites.

URL CATEGORY	CONNECTIONS	BLOCKED	DATA INBOUND (BYTES)	DATA OUTBOUND (BYTES)
Spyware and Adware	126,718		316,881,649	188,812,446
Proxy Avoid and Anonymizers	211		902,265	341,770
Phishing and Other Frauds	2,790		4,983,675	7,595,184
Malware Sites	48,922		338,237,969	70,404,658
Gross	10		46,804	6,273
Cheating	39		709,205	57,800
Keyloggers and Monitoring	11		60,518	11,460
Hacking	4		67,141	3,944
Peer to Peer	5		61,319	4,056
Social Network	1,524,896		6,942,674,933	1,178,015,274

THE APPLICATIONS ON YOUR NETWORK

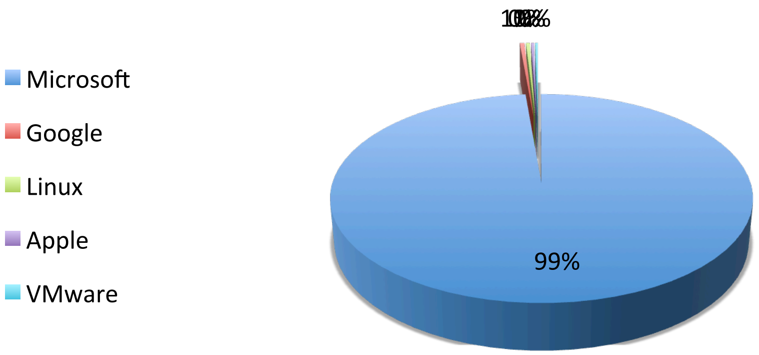
This is a list of the top applications discovered in use on your network. Three types of applications are identified and listed here: client applications (including web browsers), web applications (which run over HTTP), and server applications (for example, web servers). Full visibility over all application types enables you to get better perspective on how your networks are currently utilized.

CLIENT APPLICATIONS	WEB APPLICATIONS	SERVER APPLICATIONS
Client applications include web browsers and other desktop applications that access the network	Web applications are carried over Web-related protocols like HTTP and HTTPS. Many Web applications operate on port 80.	Server applications include web servers such as IIS and Apache
Total: 263	**Total: 975**	**Total: 109**
WSDD, Kazaa client, TFTP client, ICA client, TeamViewer…	ICQ, Facebook Apps, Skype, WebSocket, BitTorrent…	Kazaa, RDP, ICA, WSDD, IMAP…

III. ASSET PROFILE

THE OPERATING SYSTEMS ON YOUR NETWORK

The operating systems below were observed on your network. You should identify any operating systems that fall outside your IT policy and investigate them further as to whether they should be permitted.



THE MOBILE DEVICES ON YOUR NETWORK

The following mobile devices were profiled on your network. Mobile devices may be vulnerable, especially older or jailbroken versions. It is important to be aware of how mobile devices are used and set appropriate security policies.

DEVICE TYPE	VERSION	COUNT

THE FILES TRAVERSING YOUR NETWORK

	FILE CATEGORY	FILE TYPE	COUNT	PROTOCOL
DOWNLOADS	Archive	MSCAB	284,236	HTTP
	Multimedia	SWF	232,978	HTTP
	Archive	ZIP	109,330	HTTP
	PDF files	PDF	30,363	HTTP
	Multimedia	MOV	29,854	HTTP
UPLOADS	Archive	GZ	3,443	HTTP
	Archive	ZIP	401	HTTP
	PDF files	PDF	51	HTTP
	Office Documents	MSOLE2	21	HTTP
	Office Documents	NEW_OFFICE	19	HTTP
MISC	Archive	ZIP	15,790	FTP Data
	PDF files	PDF	4,170	SMTP
	Archive	7Z	3,265	FTP Data
	Office Documents	NEW_OFFICE	1,260	POP3
	Office Documents	MSOLE2	890	POP3

IV. RECOMMENDATIONS

Despite existing protections, your organization’s application usage exposes it to added risks. This assessment, which contains a profile of your network, has identified risky assets. New countermeasures and security controls are required to mitigate the risks to these assets.

Cisco recommends that FirePOWER Appliances with Application Control and URL Filtering are depoyed to:

1) Establish continuous network visibility into its application and asset risk.
2) Augment its existing controls in order to mitigate this risk

1) ESTABLISH CONTINUOUS NETWORK VISIBILITY INTO APPLICATION RISK

Existing security infrastructure provides inadequate protection against application and asset risks. Cisco recommends deployment of network-based protections via FirePOWER Appliances (NGIPS/ NGFW). These will provide the following new capabilities and benefits to augment your network visibility:

NEW CAPABILITY	BENEFIT
Network Map	Profiles hosts on the network, including network infrastructure, desktops, servers, mobile devices, virtual machines, and many others.
Application Awareness	Identifies over 1,500 applications, including client applications that run on desktops, server applications such as Web servers, and Web applications carried over HTTP. Profiles application actions, like the ability to send email or chat using a Web mail application.
Mobile Awareness	identifies and profiles mobile devices, including iOS, Android, Amazon, Blackberry, and other mobile device types. Identifies jailbroken devices.
Real-time Contextual Awareness	Profiles hosts and identifies communications that are of unusual bandwidth or hosts that are running inappropriate applications for the environment.

2) AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk applications pose. These measures may entail reduction of the application threat surface and blocking risky URLs. Cisco recommends deployment of network-based protections via FirePOWER Appliances with Application Control and URL Filtering. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Granular Application Control	Reduce potential area of attack through granular control of thousands of applications. Filter and enforce usage policy on millions of URLs.
URL Filtering	Control on a database of millions of URLs, by risk or productivity characteristics
Virtual Protection	Protect VM-to-VM communications the same as physical network

In addition, Cisco offers NGIPS capabilities and optional Advanced Malware Protection for networks and hosts, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.

ABOUT CISCO

It’s no secret that today’s advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It’s more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For nearly three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

Cisco delivers intelligent cybersecurity for the real world.

CONTACT US

Want to learn more about getting this information on your network? Go to http://cisco.com/go/security and request a live demo.

Advanced Malware Risk Report

Prepared for Company A

Tuesday 07 October 2015

Prepared by Mike Storm, Cisco Preferred Partner

Contact: partner_se@company.com

I. EXECUTIVE SUMMARY

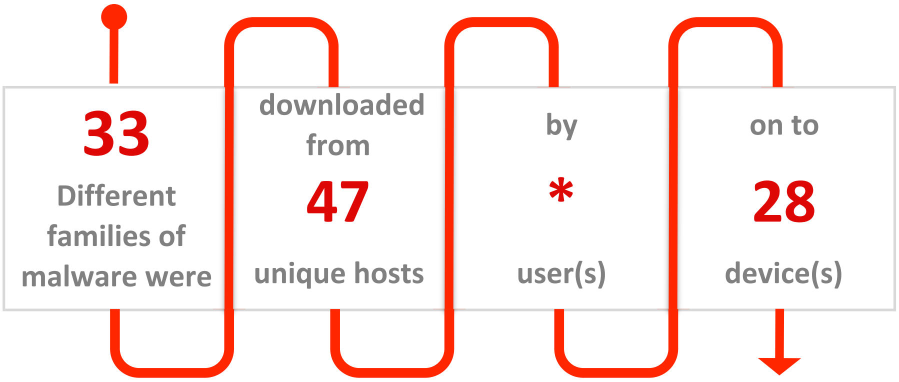
Sourcefire has determined that Company A is at a high risk due to the observation of attack by 12 different families of malware. Sourcefire Advanced Malware Protection for FirePOWER was deployed for an assessment period of 14 days. This report is a record of what was found on the network during this time

Assessment Period: Tue Sep 23 15:52:26 2014 to Tue Oct 7 15:52:26 2014

Malware Detected	**Hosts displaying IoCs**	**Infection Protocols**
189	**160**	**1**
Hosts Connected to CnC Servers	**Malware Comms**	**Malware URLs**
121	**5,790**	**40**

(A summary of the assessment results starts on page 3)

MALWARE PROFILE: OVER THE LAST 14 DAYS


33 Different families of malware were downloaded from **47** unique hosts by ***** user(s) on to **28** device(s)

*** - User mapping was not enabled in this deployment**

Cisco recommends that Advanced Malware Protection for FirePOWER is deployed to:

1. Establish continuous visibility into advanced malware
2. Augment existing controls in order to mitigate this risk

II. ASSESSMENT RESULTS

HOSTS DISPLAYING INDICATIONS OF COMPROMISE

Special attention should be paid to computers showing high amounts of indications of compromise as they are likely to be exfiltrating information from your private systems. Devices that fall into this category likely have had malware residing on them for some time already and the initial infection has been missed by existing security protections, or are under current attack.

HOST ADDRESS	IOC COUNT
10.16.252.191	3
10.236.155.254	3
10.16.5.95	2
10.236.214.131	2
10.16.217.27	2

TOTAL HOSTS CONNCTED TO BOTNET C&C SERVERS (details on next page)
121

COMMON INDICATIONS OF COMPROMISE FOUND

Indications of compromise take many forms, perhaps a host has been seen to execute malware, be connected to a Command & Control server, be targeted with a high impact attack, or actively leaking data. Across the monitored network, these are a sample of different IoCs detected against live systems.

MOST COMMON IOC TYPES DISCOVERED

IOC CATEGORY	IOC DESCRIPTION	COUNT
CnC Connected	The host may be under remote control	122
Malware Detected	The host has encountered malware	45
Exploit Kit	The host may have encountered an exploit kit	10
Impact 2 Attack	The host was attacked and is potentially vulnerable	1

HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

The following devices have been identified as being connected to command and control (CNC) servers. Cisco detects CNC detections through a blend of deep session (packet content) inspection, network communications to hosts identified by the VRT as hosting CNC infrastructure, and connections outbound from processes on an endpoint that are known to be malicious.

SAMPLE OF HOSTS CONNECTED TO CNC SERVERS

IP ADDRESS	IP ADDRESS
10.236.155.254	10.16.217.107
10.16.197.4	10.16.6.156
10.32.51.58	10.236.212.176
10.16.5.14	10.16.215.133
10.16.213.124	10.32.181.204

MALWARE FOUND ON THE NETWORK

Top threats seen in your environment should be researched because they may affect your security exposure. You should take action to remove and prevent reintroduction by these specific threat types:

FILE BASED MALWARE DETECTIONS

MALWARE NAME	NUMBER OF DETECTIONS	NUMBER OF HOSTS
W32.E4BD25F5DA-66.SBX.VIOC	34	
W32.MindsparkA.17kb.1201	36	
W32.Application:AdwareBRM.17kk.1201	16	
W32.12B308FF17-97.SBX.VIOC	6	
W32.42366A7539-100.SBX.VIOC	2	

III. FILE DETAILS

FILES SEEN MOVING AROUND THE NETWORK

The following files types have been seen moving around the network. To limit your exposure to malware risk it is wise to control data movement my policy. File movement can be controlled by user, group, network zone, app, protocol, file type, and disposition.

FILE TYPE	COUNT	MOST COMMON APPLICATION
MSCAB	284,236	HTTP
SWF	232,977	HTTP
ZIP	125,115	HTTP
PDF	32,467	HTTP
MOV	29,860	HTTP

DYNAMIC ANALYSIS & THREAT SCORE

Cisco Advanced Malware Protection (AMP) solutions provide detailed analysis of file behavior after execution takes place. A Threat Score is associated with files, this is calculated based on the behavior observed in the dynamic analysis environment.

FILENAME	SHA256	THREAT SCORE (/100)
MapsGalaxy.exe	242919…f2bf5b	100
MapsGalaxy.exe	242919…f2bf5b	100
MapsGalaxy.exe	242919…f2bf5b	100
cbsi213-Dictation_Buddy-ORG-10050668.exe	e4bd25…b6a38e	100
cbsi213-Dictation_Buddy-ORG-10050668.exe	e4bd25…b6a38e	100
cbsi213-Dictation_Buddy-ORG-10050668.exe	e4bd25…b6a38e	100
MapsGalaxy.exe	242919…f2bf5b	100
MapsGalaxy.exe	242919…f2bf5b	100
MapsGalaxy.exe	242919…f2bf5b	100
MapsGalaxy.exe	242919…f2bf5b	100

DYNAMIC ANALYSIS SUMMARY OUTPUT

Below is an example of dynamic analysis output taken from one file found on your network. This file had a threat score of 100 out of 100. A more detailed analysis of this file is available in the Defense Center along with screenshots, network traffic it generated, and files it may have also dropped.

File Sample: 242919c0d6144fc07555bcfef66c050268b5febf4a9f7737108a405f0df2bf5b
Threat Score: 100 / 100

OBSERVATION	SCORE / 100
* AV Detection	True
- Scanner Search Results	True
* E-Banking Fraud	True
- Found strings which match to known bank urls	True
* Networking	True
- Urls found in memory or binary data	True
* Persistence and Installation Behavior	100
- Drops PE files	100
* PE File Obfuscation	2
- Binary may include packed or crypted data	True
- PE sections with suspicious entropy found	10
* System Summary	35
- Binary contains paths to debug symbols	True
- Creates files inside the program directory	50
- Runs a DLL by calling functions	80
- Spawns processes	55
- Creates mutexes	10
* Anti Debugging	50
- Creates guard pages, often used to prevent reverse engineering and debugging	50

III. MALWARE RISK TO THE BUSINESS

IMPACT OF MALWARE TYPES

Malware exposes different types of risk to the organisation that encounters it. Malware is commonly categorized into different types that enable the security team to deal with the Immediate threat. Below are different types of malware commonly discovered by Cisco solutions.

MALWARE TYPE	RISK TO BUSINESS
Botnet client	Denial of Service, Information Theft. A botnet is a collection of computers controlled by a third party. Hosts controlled by a botnet may steal information from your organization or be used to launch denial-of-service attacks, send spam, or conduct other undesirable activity.
Trojan / Backdoor	System Degradation, Information Theft: A trojan horse is a program that appears to be benign to an end user but is in fact malicious. It can be used to steal information or introduce control
Spyware	Information Theft: Spyware is software installed on machines that collects information without users' knowledge and forwards it to other organizations.

IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, advanced malware is getting through and placing your organization at risk. Additional countermeasures and security controls are required to mitigate the risk.

Cisco recommends that Company A deploy FirePOWER Appliances with Advanced Malware Protection to:

1. Establish continuous network visibility into its advanced malware risk
2. Augment its existing controls in order to mitigate this risk
3. Add host protection and enhanced remediation via FireAMP connectors

1. ESTABLISH CONTINUOUS MALWARE VISIBILITY

Existing protections are neither dynamic enough nor capable of fully protecting from new or unknown threats that emerge daily. Cisco recommends deployment of network-based protections via FirePOWER Appliances with Advanced Malware Protection. Advanced Malware Protection is a license that you can add to any NGFW or NGIPS appliance from Sourcefire. This will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Network Based Detection	Detect and block advanced malware from existing network IDS/IPS infrastructure
Trend Analysis	Measure and see how effective your protections are over time
Cloud-Based Analytics	Powerful cloud analytics leverages Cisco's vast security intelligence and expertise without complex or costly deployment
Full-stack Visibility	Understand, at all architecture layers, which hosts, applications and users are involved in risky or malicious activity - use this knowledge to easily develop effective controls and inspection policies.
File Identification	Identify and understand the file types traversing your networks and employ intelligent decisions based on Cisco reputational data
Virtual Protection	Monitor VM-to-VM communications the same as physical networks

2. AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk advanced malware poses. These measures may entail control of threat surface, blocking entry and propagation of malware or suspect file types, and rapid notification upon new malware discovery.

Cisco recommends deployment of network-based protections via FirePOWER Appliances with Advanced Malware Protection. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
24/7 Real-Time Protection	Deploy in-line for continuous network protection and minimize propagation of advanced malware
IP Blacklisting	Block Bot C&C, open proxy, and custom IP lists from your IPS
Retrospective Alerting	Alert on files deemed malicious by the Cisco Security Intelligence cloud even after infection - leverage community awareness to know when you may be at risk of infection

3. ADD HOST PROTECTION & ENHANCED REMEDIATION VIA FIREAMP

Typically advanced malware enters the network via hosts (compromised end devices such as PCs, smartphones, etc.). Having a presence at the host/client-side OS enables easier determination of root cause, malware trajectory, and more control over the spread of malware (even after a compromise!). It also helps to speed post-infection clean-up efforts.

Cisco recommends considering FireAMP Advanced Malware Protection Connectors for additional visibility and control. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Host Protection	Deploy Cisco FireAMP Connectors to gain additional protection and more capability to take action against malware at the host.
Mobile Protection	Protect mobile workers and Android-based devices from advanced malware attacks
Virtual Protection	Protect Virtual Desktop communications the same as physical networks
Malware Trajectory	Understand how malware enters and trace the path of infection to identify 'patient zero'
File Analysis	Get more information on how malware behaves, the original file name, screen shots of the malware executing, and sample packet captures
Retrospective Detection	Recall files deemed malicious by the Cisco Security Intelligence cloud even after infection - automate and speed malware cleanup

In addition, Cisco offers NGIPS capabilities and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Sourcefire representative or reseller for more information.

ABOUT CISCO

Sourcefire Inc. (Nasdaq: FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize network security risks. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire provides customers with Agile Security TM that is as dynamic as the real world it protects and the attackers against which it defends.

Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with numerous patents, world- class research, and award winning technology. Today the name Sourcefire has grown synonymous with innovation, security intelligence and agile end-toned security protection.

CONTACT US

Want to learn more about getting this information on your network? Go to http://cisco.com/go/security and request a live demo.

Attack Risk Report

Prepared for Company A

Tuesday 07 October 2015

Prepared by Mike Storm, Cisco Preferred Partner

Contact: partner_se@company.com

I. EXECUTIVE SUMMARY

Cisco has determined that Company A is at a High risk due to the observation of attacks on the newtork targetting hosts that may be vulnerable. These attacks and hosts require further investigation to help lower the risk."

Assessment Period: Tue Sep 23 15:52:26 2014 to Tue Oct 7 15:52:26 2014

Total Attacks

9,586

Relevant Attacks

346

Hosts Targeted

44

Irrelevant Attacks

96.4%

Events Requiring Attention

3.6%

Hosts Connected to CnC Servers

121

(A summary of the assessment results starts on page 3)

RELEVANT ATTACKS CARRY THE FOLLOWING RISKS

RISK CLASSIFICATION	NUMBER OF EVENTS
A Network Trojan was Detected	290
Attempted Denial of Service	56

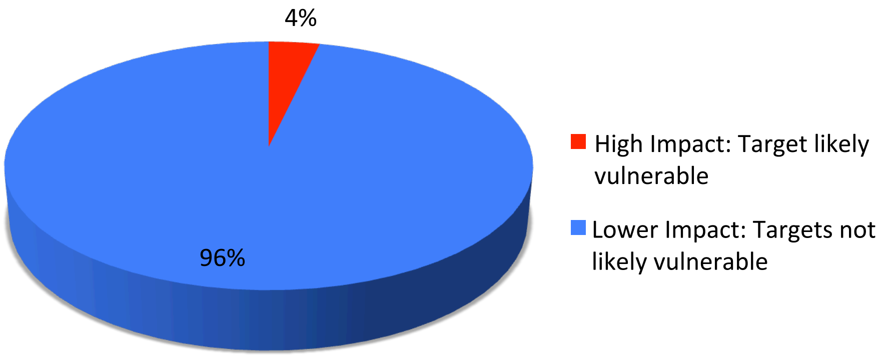
Sourcefire recommends that Company A deploy Sourcefire FirePOWER Appliances to:

1. **Establish continual visibility into its network attack risks**
2. **Implement automated protections in order to mitigate this risk going forward**

II. ASSESSMENT RESULTS

IDENTIFYING CRITICAL ATTACKS USING IMPACT ANALYSIS

Of the 9586 total attacks made on your network, 346 (3.6%) of them were considered high impact. That means that they targeted machines that were likely vulnerable to these attacks. These events are the most critical to investigate, and Cisco automatically identifies them for you. Cisco identifies high impact events automatically by correlating attacks with target risk, which is determined by passively profiling your network devices and their vulnerabilities in real time. This saves time and money over traditional solutions, which require you to qualify all events manually or import scan data from other systems.If a staff member's time is worth $75 USD per hour and each attack takes 10 seconds to qualify, then each attack costs $0.21 USD to manually qualify. The difference in qualification time and cost between Cisco and traditional solutions is substantial.



ATTACKS TO QUALIFY / YEAR	COST TO QUALIFY	COST TO QUALIFY ALL ATTACKS
250,025 estimated total attacks	0.21	52,505
9,021 estimated high impact attacks	0.21	1,894

	COST SAVINGS
Year #1	**$50,611**
Year #5	**$253,055**

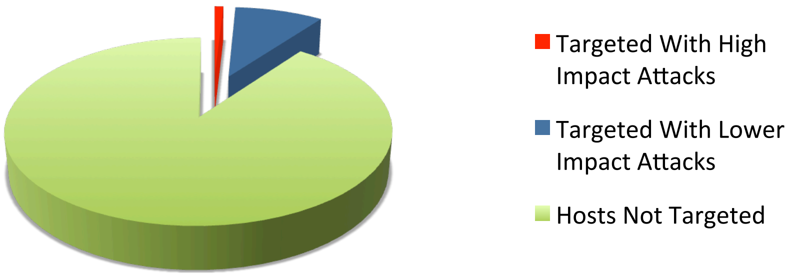
HIGH IMPACT ATTACKS

The following attacks are very important to investigate because they directly target machines that have been identified as potentially vulnerable. The target machine's operating system version, running services, and potential vulnerabilities all match what the threat is designed to attack.

EVENT TYPE	DETAILS	APPLICATION	POTENTIALLY VULNERABLE HOSTS
A Network Trojan was Detected	APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn	DNS	106.38.193.4, 111.206.63.66, 119.188.67.4,
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain counter.yadro.ru	Freenet	204.67.81.19, 204.67.186.29
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain api.wipmania.com - Troj.Dorkbot-	Freenet	204.67.186.29
A Network Trojan was Detected	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	HTTP	50.7.28.2
A Network Trojan was Detected	BLACKLIST User-Agent known malicious user-agent string SelectRebates	HTTP	72.21.81.253, 74.63.145.160, 74.63.145.172,

HOSTS AT HIGH RISK

0.9% of your hosts have been targeted with high impact attacks during the assessment period. They are at high risk of infection. The attacks should be investigated and the machines assessed to ensure that proper controls are in place. An additional 9.1% of the machines discovered on your network were targeted with some form of attack.



HOSTS ALREADY COMPROMISED

Special attention should be paid to computers already compromised by malware as they are likely to be exfiltrating information from your private systems. Systems that fall into this category likely have had malware residing on them for some time already and the initial infection has been missed by existing security protections.

SAMPLE LIST OF COMPROMISED DEVICES
10.32.185.251
10.16.213.26
10.16.37.51
10.236.111.224
10.236.212.121

TOTAL HOSTS CONNCTED TO BOTNET C&C SERVERS
121

The systems listed above are exhibiting signs of compromise as they are connecting outbound to known Command and Control (C&C) servers tracked by the Cisco Vulnerability Research Team (VRT). You should take action to remediate or restore these systems.

AUTOMATING THE TUNING EFFORT

During the assessment period the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	53,740
A new host is added to the network	1,102
A device starts using a new transport protocol	2,159
A device starts using a new network protocol	1,089

As network changes are made, Cisco solutions automatically adjust policy so that new operating systems, hosts and protocols are protected. Cisco automates the tuning process by monitoring networks in real time and observing changes, and then making appropriate policy changes as a result. For example, if Windows 2000 hosts running IIS appear on a network, Cisco ensures that rules protecting against Windows 2000 and IIS vulnerabilities, and not irrelevant rules that may cause false positives, protect these hosts.

APPLICATIONS ASSOCIATED WITH ATTACKS

The following applications have been identified as associated with attacks. You should identify applications in this list that have low business relevance and evaluate whether it would be helpful to control them on your network.

APPS ASSOCIATED WITH HIGH IMPACT EVENTS	COUNT
DNS client	236
Web browser	66
Internet Explorer	26
Freenet client	17
Chrome	1

APPS ASSOCIATED WITH LOW IMPACT EVENTS	COUNT
Internet Explorer	7,405
Web browser	1,356
DNS client	237
Windows Media Player	223
Chrome	152

TOP ATTACKERS AND TARGETS

The top attackers and target machines observed in the attack attempts on your network are listed below. For high impact attacks in particular, you should ensure that targets are well protected from potential attackers by patching these machines and blocking potentially malicious traffic.

	ATTACKERS	ATTACKS	TARGETS	ATTACKS
HIGH IMPACT EVENTS	10.16.252.210	292	204.67.186.29	192
	10.64.254.9	190	8.34.112.52	119
	10.236.155.254	141	119.188.67.4	48
	10.16.5.94	46	218.30.117.4	46
	10.16.200.103	31	203.119.29.1	39
LOWER IMPACT EVENTS	64.129.104.164	1,811	138.91.89.250	3,175
	10.227.34.44	1,649	166.90.142.110	1,064
	64.129.104.148	1,019	172.17.3.5	457
	208.76.225.74	1,005	10.64.254.9	434
	10.32.81.207	911	10.32.130.114	303

IPv6 ATTACKS AND TRAFFIC

IPv6 traffic is a potential avenue for attacks that is often left unprotected by organizations. Network security is often thought of strictly from an IPv4 perspective, yet hosts may communicate internally and even externally to an organization over IPv6, exposing them to attack risks. The following communications were observed over IPv6 during the assessment period

HOSTS USING IPv6 IN YOUR NETWORK (MONITORED)
0

ATTACKS SEEN OVER IPv6
9,586

III. BUSINESS RISK OF ATTACKS

BUSINESS RISK OF INTRUSION ATTEMPTS

Different types of attacks were detected on the Company A network, each introducing different business risks. Here are the most common attack types observed along with the risks each introduces.

ATTACK CLASSIFICATION	NUMBER OF EVENTS	RISK ASSOCIATED WITH THE ATTACK
Potential Corporate Policy Violation	5	Information Theft: These events indicate usage of apps and protocols in ways that may be prohibited by organizational policy
A Network Trojan was Detected	369	Infrastructure Damage, Information Theft: A Trojan horse is a program that appears to be benign to an end user but is in fact malicious. It can be used to steal information or cause damage.
Attempted Denial of Service	67	System Degradation, Denial of Service: Denial-of-service attacks attack the reliability of your network infrastructure, causing service to be denied to legitimate users.
Attempted Administrator/User Privilege Gain	1	Information Theft, Infrastructure Damage: Users on network machines who gain privileges illicitly may be able to steal information, control machines

IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, critical attacks are taking place and placing your organization at risk.   New countermeasures and security controls are required to mitigate the risk.

Cisco recommends deployment of network-based protections via FirePOWER NGIPS Appliances to complement existing protections. These will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Real-Time Contextual Awareness	Profile hosts, applications, users, and network infrastructure in real time. Assess potential vulnerabilities and identify network changes.
Automatic Impact Assessment	Determine the risk of any attack to your business in real time in order to optimize response to it.
Automatic Policy Tuning	Automatically tune IPS protections in response to changes in your network composition.
Association of Users with Security and Compliance Events	Associate users with activity on the network, including attacks and application usage, through integration with Active Directory servers.
Collective Intelligence	Get rapid detection and insight into emerging threats so that defenses stay effective
Virtual Protection	Protect VM-to-VM communications the same as physical networks

In addition, Cisco offers optional Advanced Malware Protection for networks and hosts, and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.

ABOUT CISCO

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It's more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For nearly three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

Cisco delivers intelligent cybersecurity for the real world.

CONTACT US

Want to learn more about getting this information on your network? Go to http://info.sourcefire.com and request a live demo.